CLAIMS

We claim:

1. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound drone traffic from a drone implanted in a network connected device and providing notice when the outbound drone traffic is detected;

a blocker for blocking the outbound drone traffic responsive to the notice provided by the outbound intrusion detection system;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device; and

a correlator for correlating the outbound trace log and the inbound trace log and deducing a source ID of an inbound message responsible for triggering the outbound drone traffic.

2. The system of claim 1, wherein the correlator instructs the blocker to block inbound traffic that bears the source ID.

3. The system of claim 1, wherein the blocker is a firewall.

4. The system of claim 1, wherein the blocker is a network router.

5. The system of claim 1, wherein the blocker is a load balancer.

6. The system of claim 1, wherein the outbound intrusion detection system provides a destination address of the outbound drone traffic to the correlator, and the correlator searches the incoming trace log for an inbound message that includes the destination address.

7. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound denial of service traffic from a drone implanted in a network connected device and providing notice when the outbound denial of service traffic is detected;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device;

a correlator for correlating the outbound trace log and the inbound trace log and deducing a source ID of an inbound message responsible for triggering the outbound denial of service traffic; and

a blocker, responsive to the notice provided by the outbound intrusion detection system, for blocking inbound traffic that bears the source ID and blocking the outbound denial of service traffic.

8. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound denial of service traffic from a drone implanted in a network connected device, providing notice when the outbound denial of service traffic is detected, and providing a destination address of the outbound denial of service traffic;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device;

a correlator for searching the inbound trace log for an inbound message that includes the destination address of the outbound denial of service traffic and determining a source ID of the inbound message that includes the destination address of the outbound denial of service traffic; and

a blocker, responsive to the notice provided by the outbound intrusion detection system, for blocking inbound traffic bearing the source ID and blocking the outbound denial of service traffic.

9. A method for detecting and controlling a drone implanted in a network connected device such as a computer, the method comprising the steps of:

monitoring outbound traffic from a network connected device for outbound drone traffic; and,

when outbound drone traffic is detected, blocking the outbound drone traffic and deducing a source ID of a message responsible for triggering the outbound drone traffic by correlating an inbound trace log and an outbound trace log.

10. The method of claim 9, further comprising the step of blocking inbound traffic that bears the source ID.

11. The method of claim 9, wherein the outbound drone traffic is blocked by a firewall.

12. The method of claim 9, wherein the outbound drone traffic is blocked by a network router.

13. The method of claim 9, wherein the outbound drone traffic is blocked by a load balancer.

14. The method of claim 9, further comprising the step of determining a destination address of the outbound drone traffic.

15. The method of claim 14, wherein the step of deducing further includes the step of searching the inbound trace log for an inbound message that includes the destination address of the outbound drone traffic.

16. A method for detecting and controlling a drone implanted in a network connected device, the method comprising the steps of:

monitoring outbound traffic from a network connected device for denial of service traffic; and,

when denial of service traffic is detected, deducing a source ID of a message responsible for triggering the denial of service traffic by correlating an inbound trace log and an outbound trace log, blocking the outbound denial of service traffic, and blocking inbound traffic that bears the source ID.

17. The method of claim 16, wherein the denial of service traffic is distributed denial of service traffic.

18. A method for detecting and controlling a drone implanted in a network connected device, the method comprising the steps of:

monitoring outbound traffic from a network connected device for outbound denial of service traffic; and,

when outbound denial of service traffic is detected, determining a destination address of the outbound denial of service traffic, deducing a source ID of a message responsible for triggering the outbound denial of service traffic by searching an inbound trace log for an inbound message that includes the destination address, blocking the outbound denial of service traffic, and blocking inbound traffic that bears the source ID.

19. The method of claim 18, wherein the denial of service traffic is distributed denial of service traffic.